BrightStor® ARCserve® Backup for Windows

Agent for Microsoft Data Protection Manager Guide

r11.5

Computer Associates®

D01239-1E

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The manufacturer of this documentation is Computer Associates International, Inc.

Contents

Chapter 1: Introducing the Agent

BrightStor® ARCserve® Backup is a comprehensive, distributed storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, business-critical applications, and network clients.

Among the agents that BrightStor ARCserve Backup offers is the BrightStor® ARCserve® Backup Agent for Microsoft Data Protection Manager (DPM). Microsoft Data Protection Manager is an integrated component of the Microsoft Windows Server System that provides data recovery with near-continuous data protection.

DPM enables disk-based data protection and recovery using Volume Shadow Copy Services to provide backup and recovery functions. DPM protects its own production servers while BrightStor ARCserve Backup backs up the DPM database and replicas, protects the DPM server, adds long term archiving capabilities, protection for applications, and bare metal disaster recovery.

Benefits of Using the Agent

The BrightStor ARCserve Backup Agent for DPM provides a comprehensive data protection solution, working with the Data Protection Manager to provide the following benefits:

DPM Server Protection

The DPM server can protect the data on many remote server systems. If the DPM server fails, the data on these remote servers is lost and cannot be recovered from the DPM server. BrightStor ARCserve Backup protects the DPM server itself and, after a failure of DPM server, you can recover the DPM server with the data backed up by BrightStor ARCserve Backup.

DPM Replica Protection

The DPM server collects file system data from DPM protected servers and stores this data on disks. Because you can only store a limited number of versions of files on the DPM server, BrightStor ARCserve Backup allows you to move this data from the DPM server to disk arrays or tape libraries and make it available for restore to the DPM server or directly to the DPM file agent system.

Long Term Archiving

The agent provides the ability to archive data on tapes for disaster recovery and regulatory compliance. The agent can move data protected by DPM to tapes, archiving disks, or Virtual Tape Libraries (VTL) storage systems. BrightStor ARCserve Backup encryption ensures that the data on the tapes cannot be misused even if the tapes are accessed inappropriately.

Bare Metal Disaster Recovery

The agent provides fast and efficient file recovery. However, in the event of a total server crash, the server must be reconfigured and reinstalled before DPM can restore files, increasing recovery time significantly. Using the BrightStor® ARCserve® Backup Disaster Recovery Option with the Agent for Microsoft DPM, you can reduce recovery time after DPM server failure.

Direct Recovery of Archived Files

The agent provides improved restore time for files residing on the DPM server, allowing fast recovery of files archived to tape when restoring them to the DPM server or the originating DPM protected server.

How the Agent Works

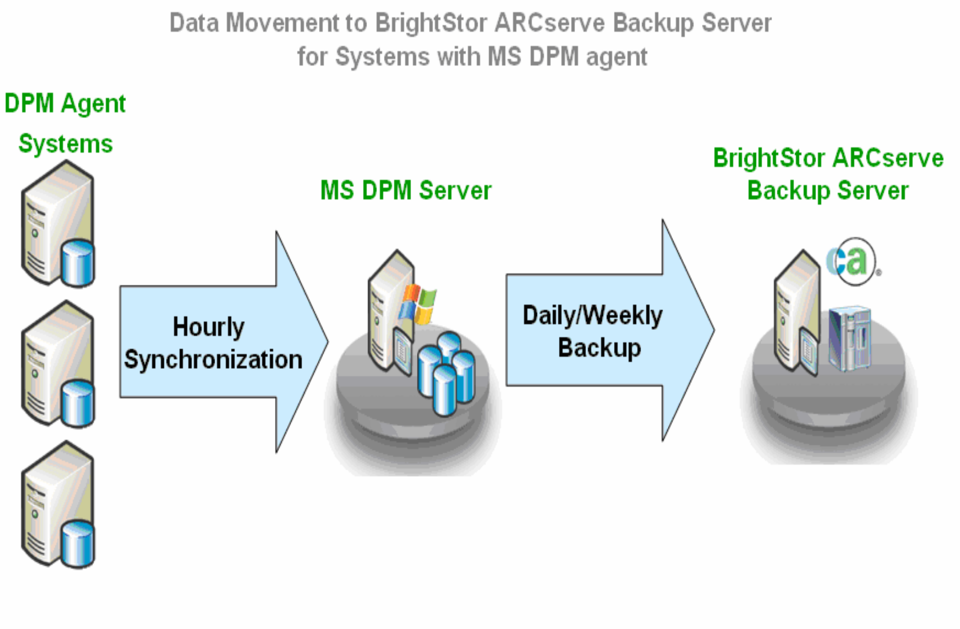
The agent protects Microsoft Data Protection Manager databases and replicas by backing them up to the BrightStor ARCserve Backup server.

The agent performs the following tasks:

- Browses and selects the items for backup
- Runs backup jobs
- Writes data to backup media
- Stores necessary information in the BrightStor ARCserve Backup database
- Browses and selects items for restore
- Executes restore jobs
- Retrieves data from the backup media and restores it to disk

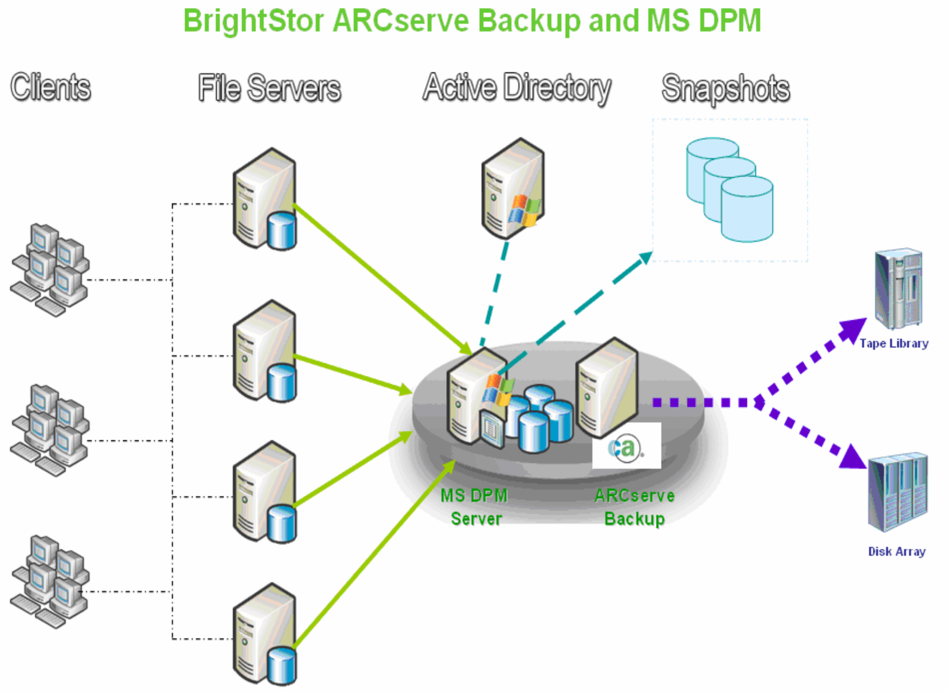
The Agent for DPM integrates with the DPM server to deliver data protection, long term archiving capabilities, protection for applications, and feature rich disaster recovery capabilities. Using the Microsoft Volume Shadow Copy Service (VSS) infrastructure, the agent takes snapshots of the DPM server, including the DPM database and replicas, and then backs up the snapshots to tape or disk devices. You back up your data from the replicas on the DPM server rather than from the live data on the DPM protected servers. Because you back up from a read-only snapshot of the data, you can run backup jobs at any time without affecting the performance of DPM protected servers. With BrightStor ARCserve Backup and the agent, you can restore DPM-archived data directly from your archive media to your DPM protected server without involving the DPM server.

The data flow between BrightStor ARCserve Backup, the agent and DPM is illustrated in the following figure:



Architecture

BrightStor ARCserve Backup can be installed on the same system as the DPM server to back up DPM data and configuration information locally or can be installed remotely to back up multiple DPM servers over the network. Remote backup performance can be affected if the DPM server has a very large amount of data, because network bandwidth may limit the transfer of data to the backup server. With local backup, the tape drive or virtual tape library (VTL) on which the data is archived is directly connected to the DPM server. If the DPM server and BrightStor ARCserve Backup are installed in the same system, DPM data can be moved directly to tape from the disk, bypassing the network.



Components

The BrightStor ARCserve Backup DPM data protection solution contains the following components:

BrightStor ARCserve Backup

> Protects mission-critical database applications and systems using application agents and the Client Agent for Windows, by backing up to disk arrays, tape libraries and VTLs.

BrightStor ARCserve Backup Agent for Microsoft DPM

This protection agent, installed on the server running Microsoft DPM, is used by BrightStor ARCserve Backup to protect Microsoft DPM.

BrightStor® ARCserve® Backup Client Agent for Windows

Backs up system state information and performs bare metal recovery of the server and restores files directly from the backup server to the DPM protected server. Because Microsoft DPM agents cannot back up system state configuration information, Microsoft DPM backups can not be used for bare metal recovery. These functionalities work even if the DPM server is offline, so, if the DPM server crashes, you can restore file system data directly from the BrightStor ARCserve Backup server.

Note: One or more of the above components can be on the same server.

Service Roles

For a DPM backup to be successful, the following entities must work together and with VSS to prepare and perform the backup:

- Requestors
- Providers
- Writers
- Components

Requestors

The Requestor is a piece of software (typically a backup application) responsible for the following tasks:

- Initiating the request for a DPM backup
- Processing the backup instructions from the Writers, including which files should be included for backup when a component is selected and the methods that should be used to back up and restore those files
- Backing up the shadow copy data to media
- Signaling the completion of the backup by deleting the shadow copy data from the disk

BrightStor ARCserve Backup is designed to function as the Requestor in DPM backups.

Providers

The Provider is responsible for managing the volumes involved in the shadow copy backup, as well as for creating the shadow copy. The Provider interfaces with the shadow copy creation capabilities that are either part of the operating system (software-based) or on the disk array (hardware-based).

Hardware disk array vendors can supply their own Providers to interface with the VSS framework, and direct where and how to create the shadow copies.

There are two types of Providers - software-based and hardware-based.

- Software-based Providers are typically implemented as a DLL and a filter to manage storage. The shadow copies are created by the software. Shadow copies created with this type of Provider include a point-in-time view of the original volume as it existed before the shadow copy, and the subsequent snapshots of only the changed data.
- Hardware-based Providers are implemented at the hardware level and work with a hardware controller or storage adapter. Shadow copies are created by a storage appliance, host adapter, or RAID device outside the operating system. Shadow copies created with a hardware-based Provider are of an entire volume (a full copy), and are typically mirrored views of the original volume. Additionally, if a transportable shadow copy is created, it can be imported onto other servers within the same system.

Writers

A Writer is part of a VSS-aware application or service that participates in a backup in the following ways:

- Works with VSS to prepare the application or service’s data to be frozen
- Suspends writes to the original volume while the shadow copy is created
- Supplies a list of Components to include in the backup (and the restore) to VSS and the Requestor

To ensure that the data used to create the shadow copy is internally consistent, VSS informs the applications or services that control the files included in the backup to freeze. When an application or service is frozen, the state of the files under its control is consistent. It is the responsibility of the Writer to let VSS know when an application or service’s files are in a consistent state.

To ensure that this state does not change during the creation of a shadow copy, the Writers suspend the ability of the application or service to make changes to the volume serving as the source of the shadow copy. The application or service Writer ensures the consistency of its data at the time of the creation of the shadow copy. Work can continue as usual on the original volume, but no changes are actually made to the data until after the shadow copy has been created.

A Writer is also responsible for supplying a list of Components to VSS and to the Requestor in the form of a writer metadata document. A writer metadata document is an XML file produced by a Writer that contains instructions for the Requestor, such as which Components are to be backed up, the backup and restore methods to be used, and a list of any files that should be excluded from the backup.

Note: BrightStor ARCserve Backup does not support Writers under Windows XP. This is because some of the necessary Writer support in Windows Server 2003 is not included in the Windows XP operating system.

Components

A Component is a group of files treated as a single unit by the Writers. The files that make up a Component are grouped together because they are mutually dependent on one another. For example, in a database, each file serves an important function in the context of the database as a whole, but on its own, a single file from a database has no use. By grouping all of these essential files into a Component, you ensure that all the data needed to successfully back up an application and its related files is backed up and can be restored later. If any of the files comprising a Component are inaccessible when the shadow copy is being created, the backup of the Component will fail.

Contact Customer Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Customer Support at http://ca.com/support.

Chapter 2: Installing the Agent

This chapter provides information to help you install the Agent for Microsoft Data Protection Manager on Windows platforms. The information in this chapter assumes you are familiar with the characteristics and requirements of Windows Server 2003 and Microsoft Data Protection Manager 2006 in general, and with the administrator responsibilities in particular.

When the agent is installed, you can begin your first Microsoft DPM backup. No further configuration is necessary to use the agent to back up and restore Microsoft DPM.

Prerequisites

Before you install the Agent for Microsoft Data Protection Manager, verify that you meet following prerequisites:

- Your system configuration meets the minimum requirements needed to install the agent

  For a list of these requirements, see the readme file

- You have administrator privileges or the proper authority to install software on the machine on which you are installing the agent

  Note: Contact your BrightStor ARCserve Backup administrator to obtain the proper rights if you do not have them.

- You have installed the Server and Manager for this release of BrightStor ARCserve Backup for Windows on the backup host

  Note: You must install the agent on the same host as the Data Protection Manager that you want to back up.

- You have the name and password of the machine on which you are installing the agent

Licensing

To use the agent, you must enter the license for the agent on the backup server you want to use to protect the Data Protection Manager. The backup server verifies that the agent is licensed.

For more information about licensing, see the *Getting Started* guide.

Installation Considerations

You can install the BrightStor ARCserve Backup server or the BrightStor ARCserve Backup Client Agent for Windows on the same machine as Microsoft DPM.

You must install BrightStor ARCserve Backup Agent for Microsoft DPM on the same machine on which the BrightStor ARCserve Backup server or client agent is installed to back up Microsoft DPM.

Agent Installation

Install the agent on each Data Protection Manager server you want BrightStor ARCserve Backup to back up.

The agent follows the standard installation procedure for the system components, agents, and options of BrightStor ARCserve Backup. For the detailed steps in this procedure, see the *Getting Started* guide.

Chapter 3: Using the Agent

This chapter provides information about the procedures and options you can use to back up or restore your data using the BrightStor ARCserve Backup Agent for Microsoft DPM. For an overall description of backup features, see the *Administrator Guide*.

Backup Operations

You must have BrightStor ARCserve Backup Agent for Microsoft DPM installed on a machine that has either the BrightStor ARCserve Backup Server component or the BrightStor ARCserve Backup Client Agent for Windows to back up Microsoft DPM data.

Backup Options

When you select a DPM server for backup, standard BrightStor ARCserve Backup options are available.

Add Remotely- Installed DPM Server

If the Client Agent for Windows (not BrightStor ARCserve Backup Server component) is installed on the same server as Microsoft DPM, perform the following steps to add **the remotely-installed DPM server to BrightStor ARCserve Backup as a backup source:**

1. On the Backup Manager Source tab, right-click Windows NT/2000/XP/2003 Systems in the displayed tree.
2. Select Add Machine/Object from the pop-up menu.

   The Add Agent dialog appears.
3. Enter the host name and IP address of your DPM server. If you do not have an IP address, click the Use Computer Name Resolution box.
4. Click Add.

   The server is registered with BrightStor ARCserve Backup.

Back Up DPM Data

To protect your Microsoft DPM, you can back up Microsoft System Center Data Protection Manager 2006 Writers. Alternatively, you can back up only the DPM database or the DPM replica.

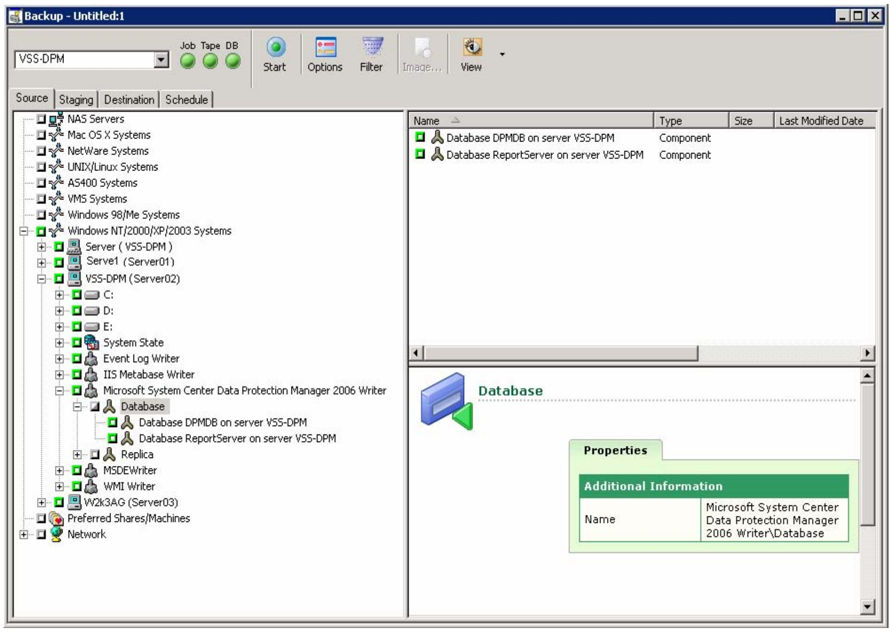
Select a Microsoft System Center Data Protection Manager 2006 Writer, DPM database or DPM replica from the tree on the Source tab of the Backup Manager to protect Microsoft DPM data. DPM replica backup operations back up data at the file or directory level.

Back Up DPM Databases

Use the following steps to back up a DPM database:

1. Expand Microsoft System Center Data Protection Manager 2006 Writer on the Backup Manager Source tab.

   The available databases appear.



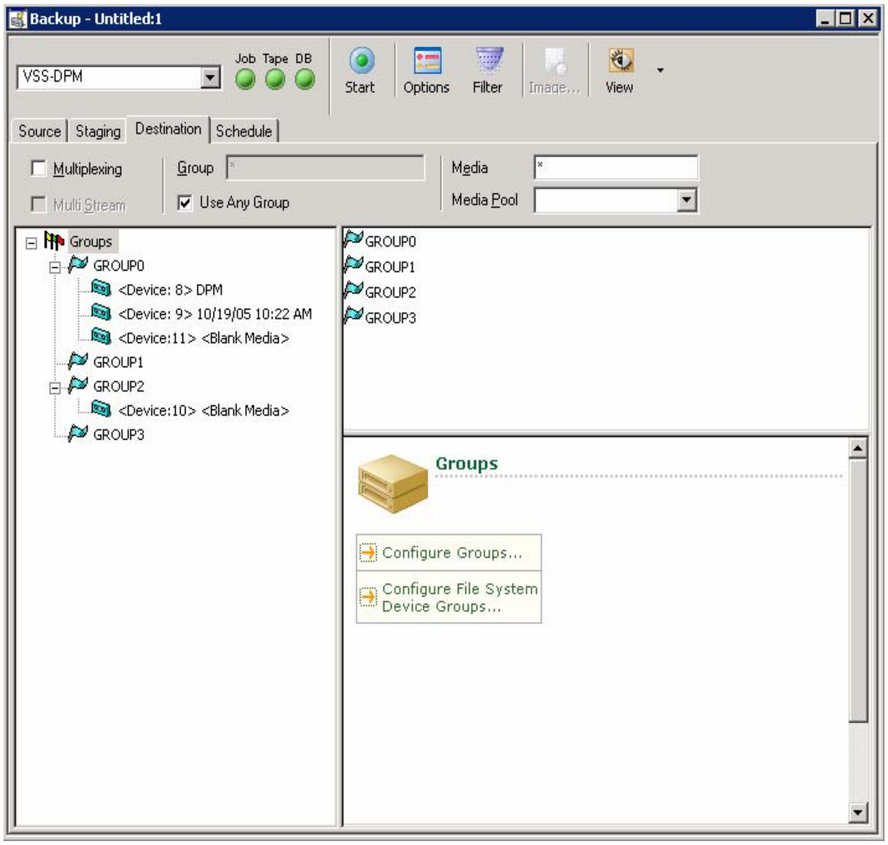
Name	Type	Size	Last Modified Date
Database DPMDB on server VSS-DPM	Component		
Database ReportServer on server VSS-DPM	Component		

Additional Information

Name	Microsoft System Center Data Protection Manager 2006 Writer\Database

2. Click the appropriate green box next to the DPM database you want to back up.

3. Select the target device for your backup job on the Destination tab.



VSS-DPM

☐ Multiplexing

☐ Multi Stream

Group *

☑ Use Any Group

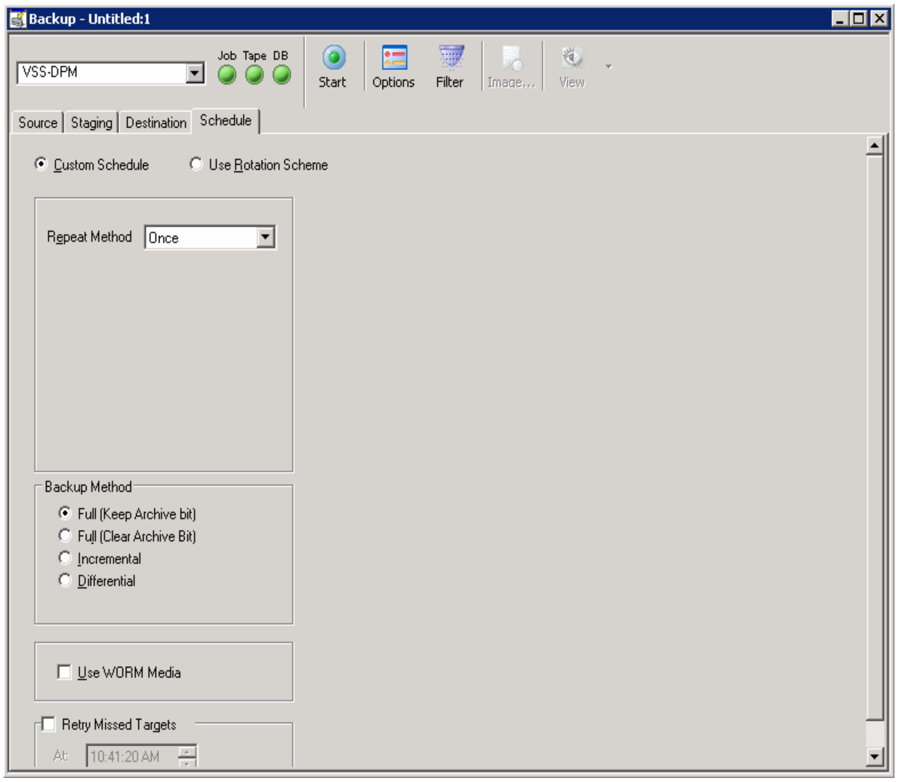
Media *

Media Pool

- Groups
  - GROUP0
    - <Device: 8> DPM
    - <Device: 9> 10/19/05 10:22 AM
    - <Device:11> <Blank Media>
  - GROUP1
  - GROUP2
    - <Device:10> <Blank Media>
  - GROUP3

GROUP0
GROUP1
GROUP2
GROUP3

4. Select the appropriate method from the Repeat Method drop-down list on the Schedule tab.



● Custom Schedule ○ Use Rotation Scheme

Repeat Method: Once

Backup Method
- ● Full (Keep Archive bit)
- ○ Full (Clear Archive Bit)
- ○ Incremental
- ○ Differential

□ Use WORM Media

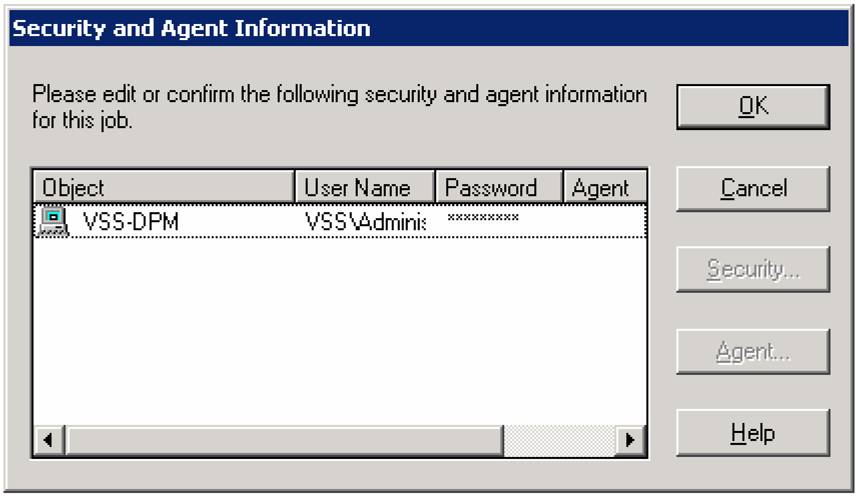
□ Retry Missed Targets

At: 10:41:20 AM

Note: Incremental and Differential Backup Methods are not supported for backing up DPM Writers. Backup jobs are always Full Backup.

5. Click Start.

   The Security and Agent Information dialog appears.



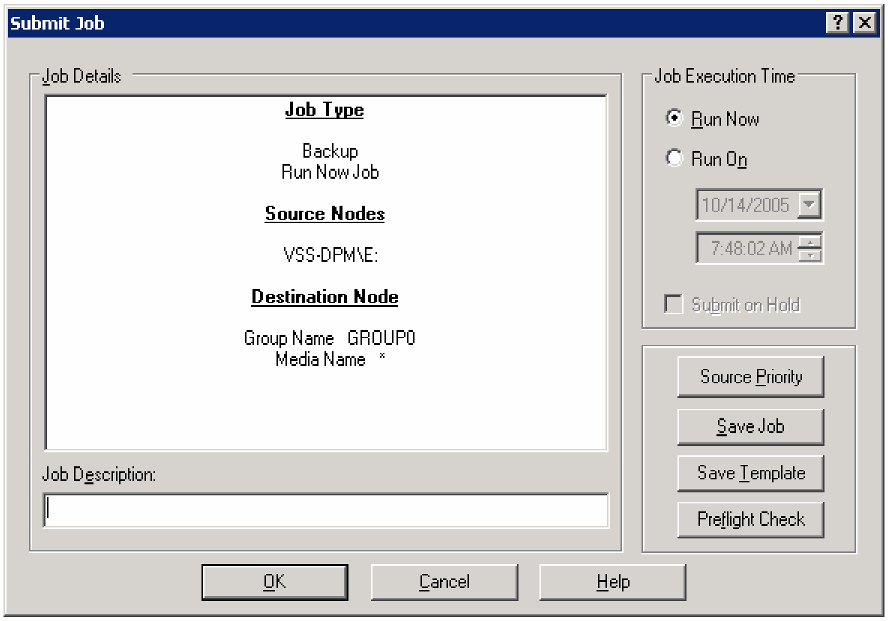
Security and Agent Information

Please edit or confirm the following security and agent information for this job.

Object	User Name	Password	Agent
VSS-DPM	VSS\Adminis	**********	

6. Edit or confirm the information in the Security and Agent Information dialog and click OK.

   The Submit Job dialog appears.



Submit Job

Job Details

Job Type

Backup
Run Now Job

Source Nodes

VSS-DPM\E:

Destination Node

Group Name GROUP0
Media Name *

Job Description:

Job Execution Time

● Run Now

○ Run On

10/14/2005

7:48:02 AM

□ Submit on Hold

7. Select the appropriate Job Execution Type. You can select one of the following:

   - **Run Now:** The backup job starts immediately
   - **Run On:** Enter the date and time to start the backup job

8. Click OK.

   You can monitor the job's progress using the Job Status Manager.

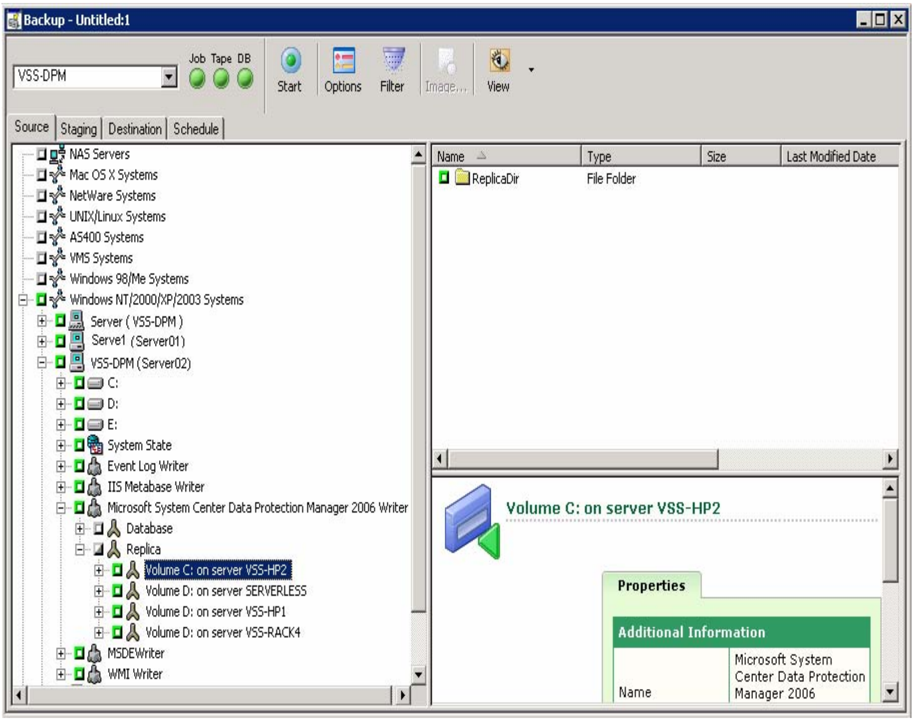
   Note: For more information about the Job Status Manager, see the *Administrator Guide*.

Back Up DPM Replicas

Use the following steps to back up a DPM replica:

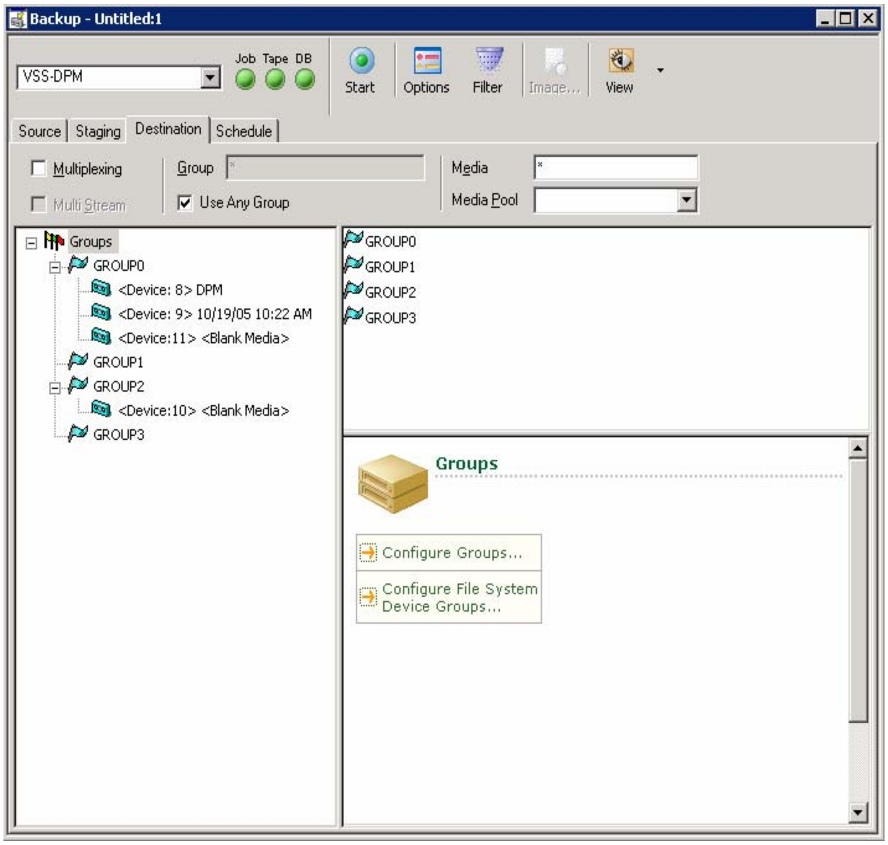
1. Expand the Microsoft System Center Data Protection Manager 2006 Writer on the Backup Manager Source tab.

   The replicas on the DPM server appear. You can back up individual files and folders or entire replicas.



2. Select the files, folders, or replica to back up.

3. Select the target device for your backup job on the Destination tab.



☐ Multiplexing

☐ Multi Stream

Group *

☑ Use Any Group

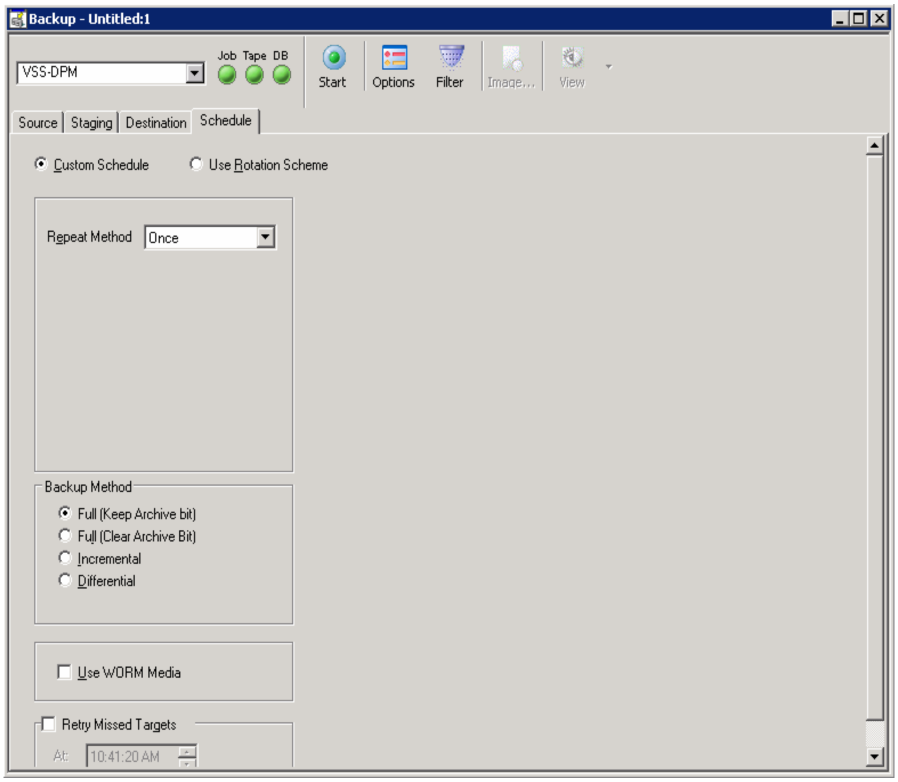
Media *

Media Pool

- Groups
  - GROUP0
    - <Device: 8> DPM
    - <Device: 9> 10/19/05 10:22 AM
    - <Device:11> <Blank Media>
  - GROUP1
  - GROUP2
    - <Device:10> <Blank Media>
  - GROUP3

GROUP0
GROUP1
GROUP2
GROUP3

4. Select the appropriate method from the Repeat Method drop-down list on the Schedule tab.



VSS-DPM

● Custom Schedule ○ Use Rotation Scheme

Repeat Method: Once

Backup Method

● Full (Keep Archive bit)

○ Full (Clear Archive Bit)

○ Incremental

○ Differential

□ Use WORM Media

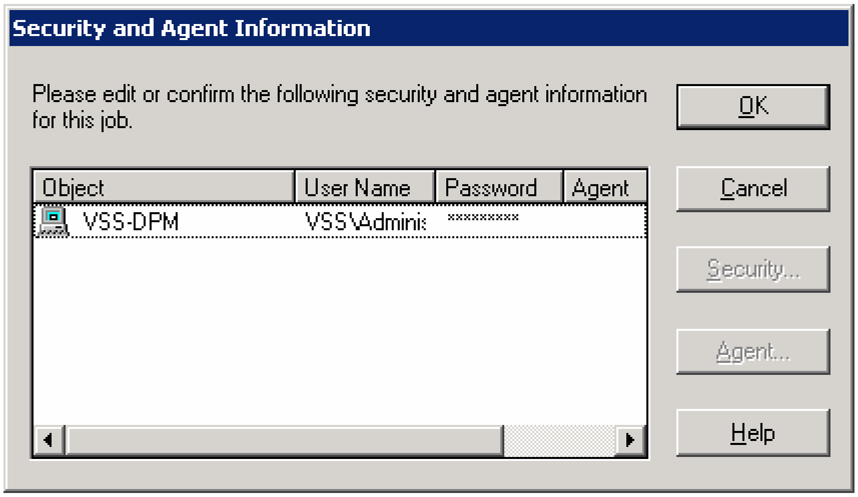
□ Retry Missed Targets

At: 10:41:20 AM

Note: Incremental and Differential Backup Methods are not supported for backing up the DPM Writer. Backup jobs are always Full Backup.

5. Click Start.

The Security and Agent Information dialog appears.

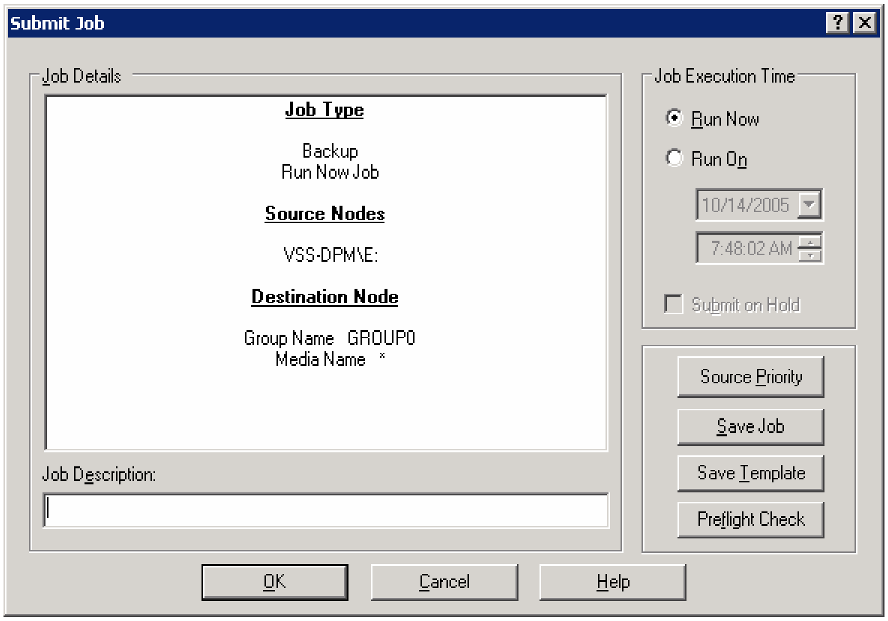


Please edit or confirm the following security and agent information for this job.

Object	User Name	Password	Agent
VSS-DPM	VSS\Adminis	**********	

6. Edit or confirm the information in the Security and Agent Information dialog and click OK.

   The Submit Job dialog appears.



Submit Job

Job Details

Job Type

Backup
Run Now Job

Source Nodes

VSS-DPM\E:

Destination Node

Group Name GROUP0
Media Name *

Job Description:

Job Execution Time

● Run Now

○ Run On

10/14/2005

7:48:02 AM

□ Submit on Hold

7. Select the appropriate Job Execution Type. You can select one of the following:

   - **Run Now:** The backup job starts immediately
   - **Run On:** Enter the date and time to start the backup job

8. Click OK.

   You can monitor the job's progress using the Job Status Manager.

   Note: For more information about the Job Status Manager, see the *Administrator Guide*.

Restore Operations

You can restore data to its original location, a location on DPM server, or to a location on a remote machine.

Restore Methods

The restore methods for the agent are available in a drop-down list on the Source tab of the Restore Manager. When a DPM server is selected for restore, the available methods are:

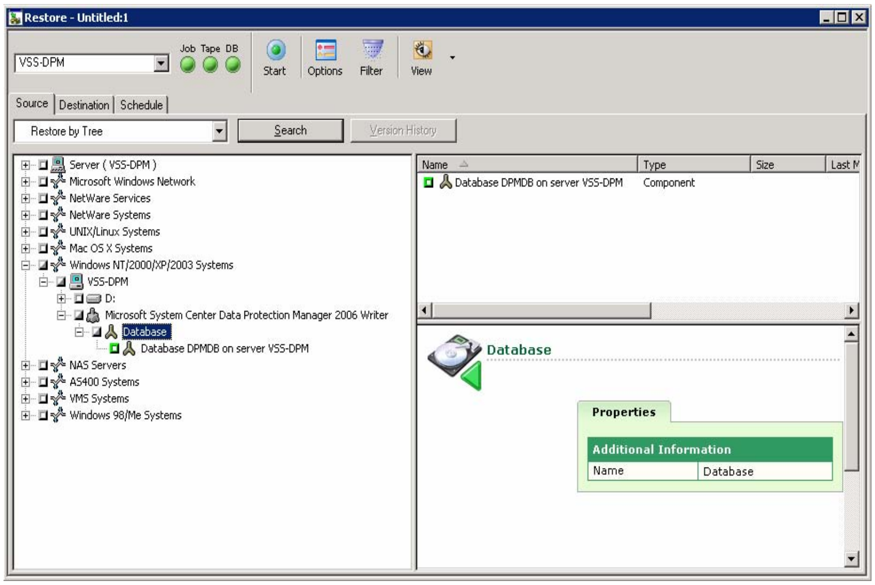
- **Restore By Tree**—The Restore By Tree method lets you select objects for restore jobs based on the source machine from which the data was backed up. If you select this method, you cannot restore the entire contents of the server as a whole but instead must select all subordinate objects individually. Use this method when you do not know which media contains the data you need but you have a general idea of what you need to restore and which machine it came from. It is the default method for the Restore Manager.
- **Restore By Session**—The Restore By Session method displays a list of all media used in backups and the files contained on them. This method lets you select objects for restore jobs based on backup sessions.

Restore Using the Restore by Tree Method

Use the following steps to restore using the Restore by Tree method:

1. Select the Restore by Tree method on the Restore Manager Source tab.
2. Expand the computer from which the DPM Writer was backed up in the navigation tree.

   The DPM Writer components available for restore are displayed.

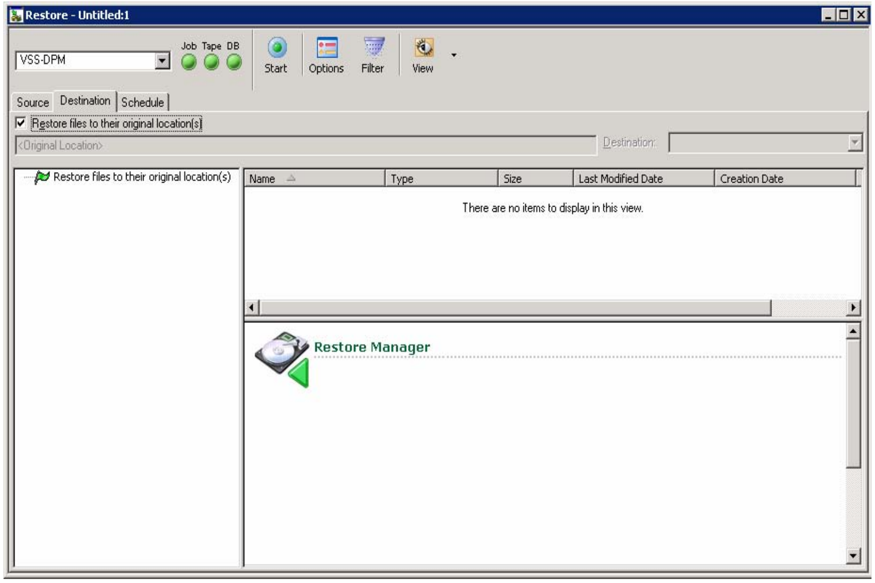


Name	Type	Size	Last M
Database DPMDB on server VSS-DPM	Component		

Additional Information	
Name	Database

3. Click the appropriate green box next to the DPM Writer component you want to restore.

4. Select the target path for your restore job on the Destination tab.



VSS-DPM

☑ Restore files to their original location(s)

<Original Location>

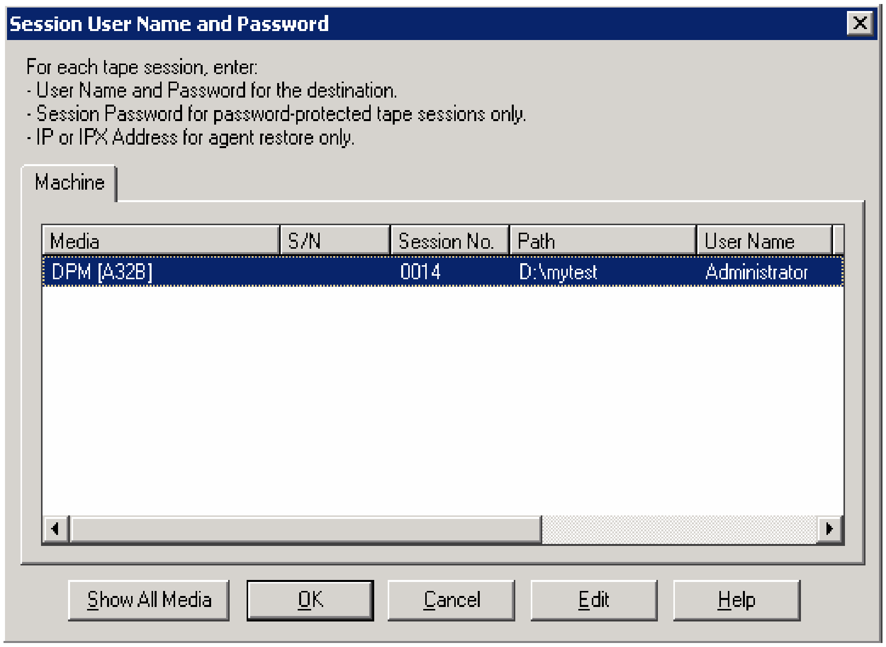
Restore files to their original location(s)

Name	Type	Size	Last Modified Date	Creation Date

There are no items to display in this view.

5. Click Start.

The Session User Name and Password dialog appears.

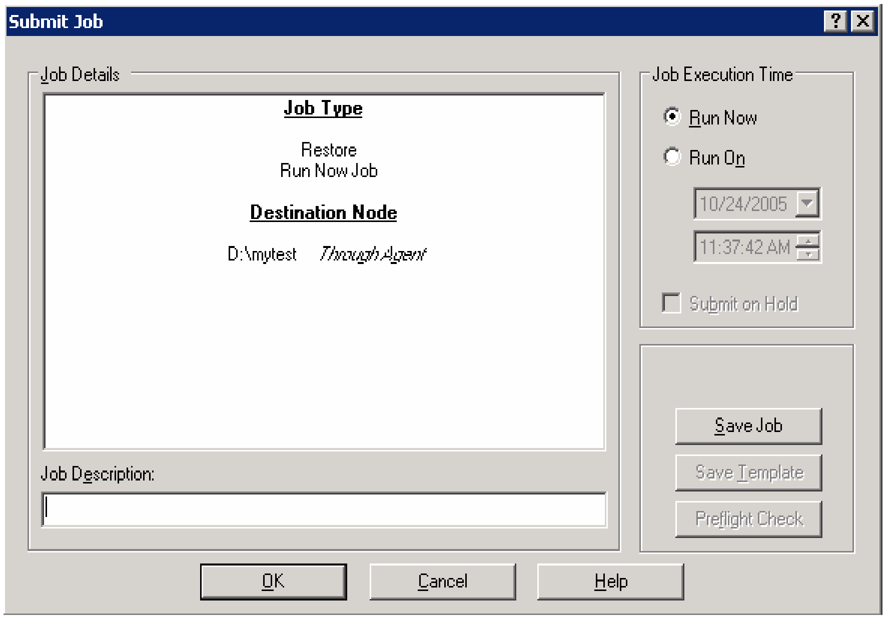


For each tape session, enter:
- User Name and Password for the destination.
- Session Password for password-protected tape sessions only.
- IP or IPX Address for agent restore only.

Media	S/N	Session No.	Path	User Name
DPM [A32B]		0014	D:\mytest	Administrator

6. Edit or confirm the information in the Session User Name and Password dialog and click OK.

   The Submit Job dialog appears.



Submit Job

Job Details

Job Type

Restore
Run Now Job

Destination Node

D:\mytest *Through Agent*

Job Description:

Job Execution Time

● Run Now

○ Run On

10/24/2005

11:37:42 AM

□ Submit on Hold

7. Select the appropriate Job Execution Type. You can select one of the following:

   - **Run Now:** The restore job starts immediately
   - **Run On:** Enter the date and time to start the restore job

8. Click OK.

   You can monitor the job's progress using the Job Status Manager.

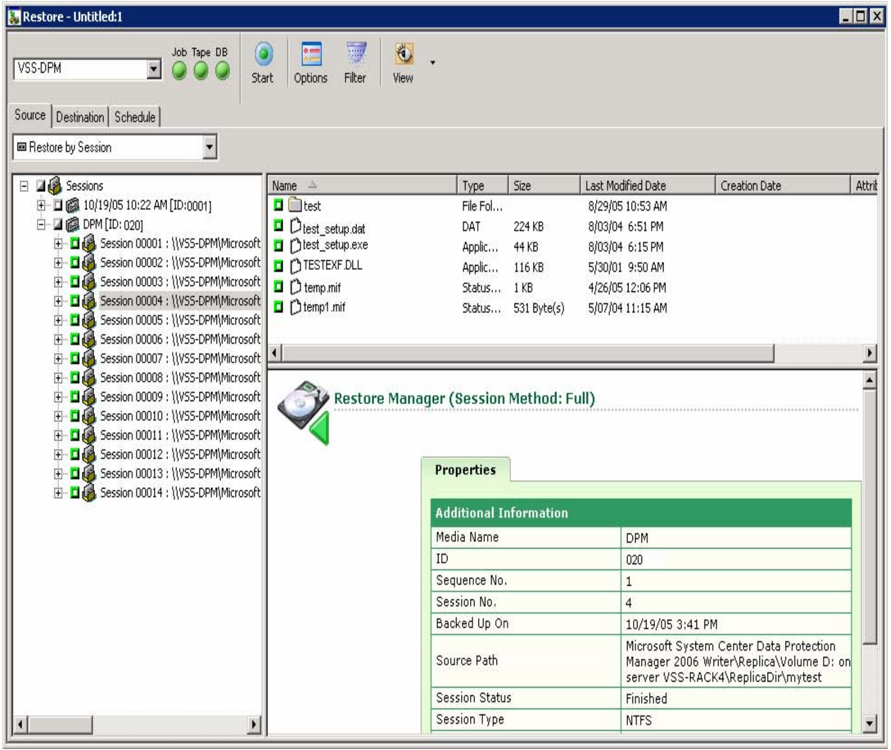
   Note: For more information about the Job Status Manager, see the *Administrator Guide*.

Restore Using the Restore by Session Method

Use the following steps to restore using the Restore by Session method:

1. Select the Restore by Session method on the Restore Manager Source tab.

   A list of sessions you have backed up with BrightStor ARCserve Backup are displayed.

   - Sessions
     - 10/19/05 10:22 AM [ID:0001]
     - DPM [ID: 020]
       - Session 00001 : \\VSS-DPM\Microsoft
       - Session 00002 : \\VSS-DPM\Microsoft
       - Session 00003 : \\VSS-DPM\Microsoft
       - Session 00004 : \\VSS-DPM\Microsoft
       - Session 00005 : \\VSS-DPM\Microsoft
       - Session 00006 : \\VSS-DPM\Microsoft
       - Session 00007 : \\VSS-DPM\Microsoft
       - Session 00008 : \\VSS-DPM\Microsoft
       - Session 00009 : \\VSS-DPM\Microsoft
       - Session 00010 : \\VSS-DPM\Microsoft
       - Session 00011 : \\VSS-DPM\Microsoft
       - Session 00012 : \\VSS-DPM\Microsoft
       - Session 00013 : \\VSS-DPM\Microsoft
       - Session 00014 : \\VSS-DPM\Microsoft

Name	Type	Size	Last Modified Date	Creation Date	Attrit
test	File Fol...		8/29/05 10:53 AM		
test_setup.dat	DAT	224 KB	8/03/04 6:51 PM		
test_setup.exe	Applic...	44 KB	8/03/04 6:15 PM		
TESTEXF.DLL	Applic...	116 KB	5/30/01 9:50 AM		
temp.mif	Status...	1 KB	4/26/05 12:06 PM		
temp1.mif	Status...	531 Byte(s)	5/07/04 11:15 AM		

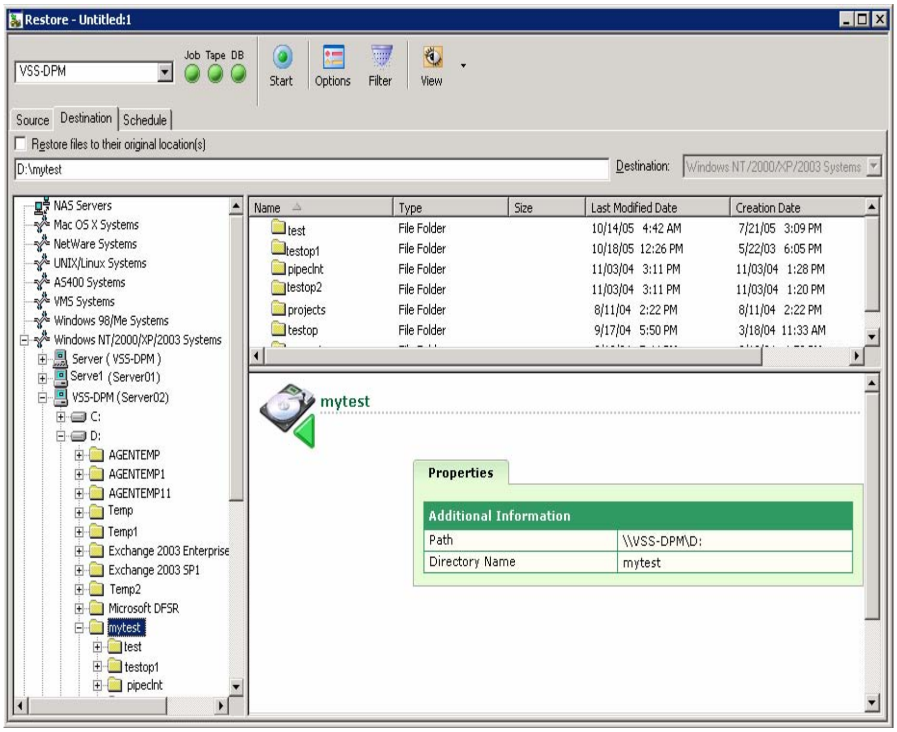
   Restore Manager (Session Method: Full)

   Properties

Additional Information	
Media Name	DPM
ID	020
Sequence No.	1
Session No.	4
Backed Up On	10/19/05 3:41 PM
Source Path	Microsoft System Center Data Protection Manager 2006 Writer\Replica\Volume D: on server VSS-RACK4\ReplicaDir\mytest
Session Status	Finished
Session Type	NTFS

2. Click the appropriate green box next to the session you want to restore.

3. Select the target path for your restore on the Destination tab.



□ Restore files to their original location(s)

D:\mytest

Destination: Windows NT/2000/XP/2003 Systems

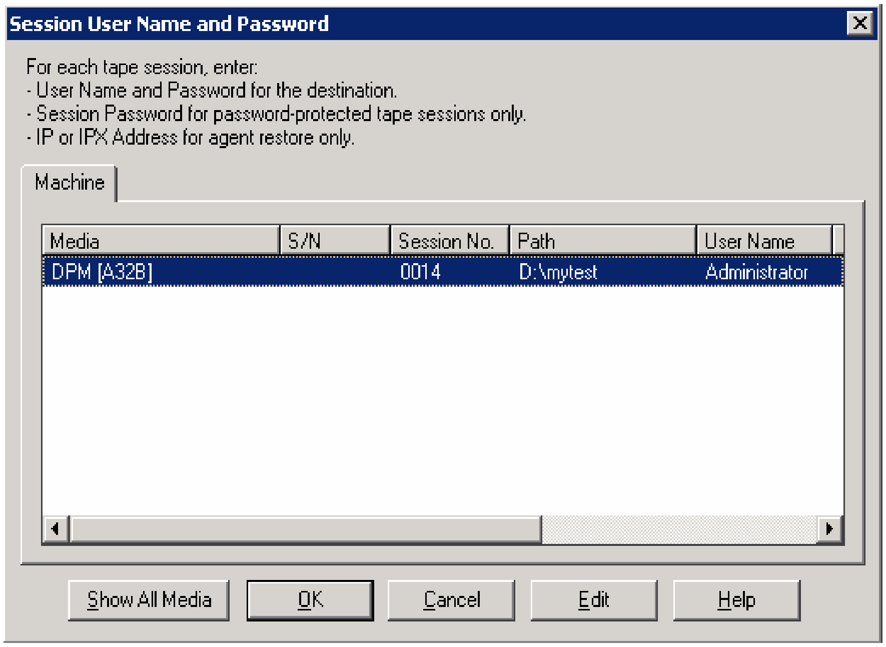
Name	Type	Size	Last Modified Date	Creation Date
test	File Folder		10/14/05 4:42 AM	7/21/05 3:09 PM
testop1	File Folder		10/18/05 12:26 PM	5/22/03 6:05 PM
pipeclnt	File Folder		11/03/04 3:11 PM	11/03/04 1:28 PM
testop2	File Folder		11/03/04 3:11 PM	11/03/04 1:20 PM
projects	File Folder		8/11/04 2:22 PM	8/11/04 2:22 PM
testop	File Folder		9/17/04 5:50 PM	3/18/04 11:33 AM

Properties

Additional Information	
Path	\\VSS-DPM\D:
Directory Name	mytest

4. Click Start.

The Session User Name and Password dialog appears.

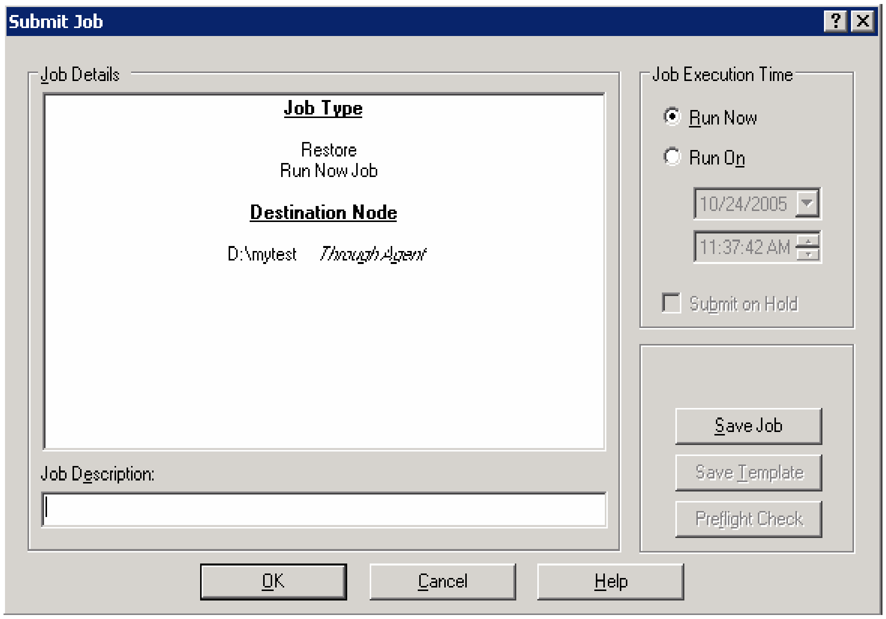


For each tape session, enter:
- User Name and Password for the destination.
- Session Password for password-protected tape sessions only.
- IP or IPX Address for agent restore only.

Media	S/N	Session No.	Path	User Name
DPM [A32B]		0014	D:\mytest	Administrator

5. Edit or confirm the information in the Session User Name and Password dialog and click OK.

   The Submit Job dialog appears.



Job Type

Restore
Run Now Job

Destination Node

D:\mytest *Through Agent*

● Run Now

○ Run On

10/24/2005

11:37:42 AM

□ Submit on Hold

6. Select the appropriate Job Execution Type. You can select one of the following:

   - **Run Now:** The restore job starts immediately
   - **Run On:** Enter the date and time to start the restore job

7. Click OK.

   You can monitor the job's progress using the Job Status Manager.

   Note: For more information about the Job Status Manager, see the *Administrator Guide*.

Recovery Scenarios

The following types of data loss can affect your DPM data:

- Loss of individual files
- Loss of a DPM protected server
- Loss of the DPM server
- Loss of DPM and DPM protected servers
- Loss of the BrightStor ARCserve Backup Server

The following section discusses each type of failure and how to recover from it.

Individual File Loss

The loss of individual files or volumes protected by DPM servers can happen in the following ways:

- Loss of files or volumes from the DPM server
- Loss of files or volumes archived to the BrightStor ARCserve Backup server

Loss of Files From the DPM Server

If you have lost files from the DPM server, you can recover these files from the DPM server (you must have DPM administrator rights or be an end-user with end-user recovery enabled). Use Windows Explorer or Microsoft Office 2003 to access the DPM shadow copies from your workstations and recover point-in-time copies of the files.

See the *Microsoft Data Protection Manager Planning and Deployment Guide* for more information.

Loss of Files Moved to the BrightStor ARCserve Backup Server

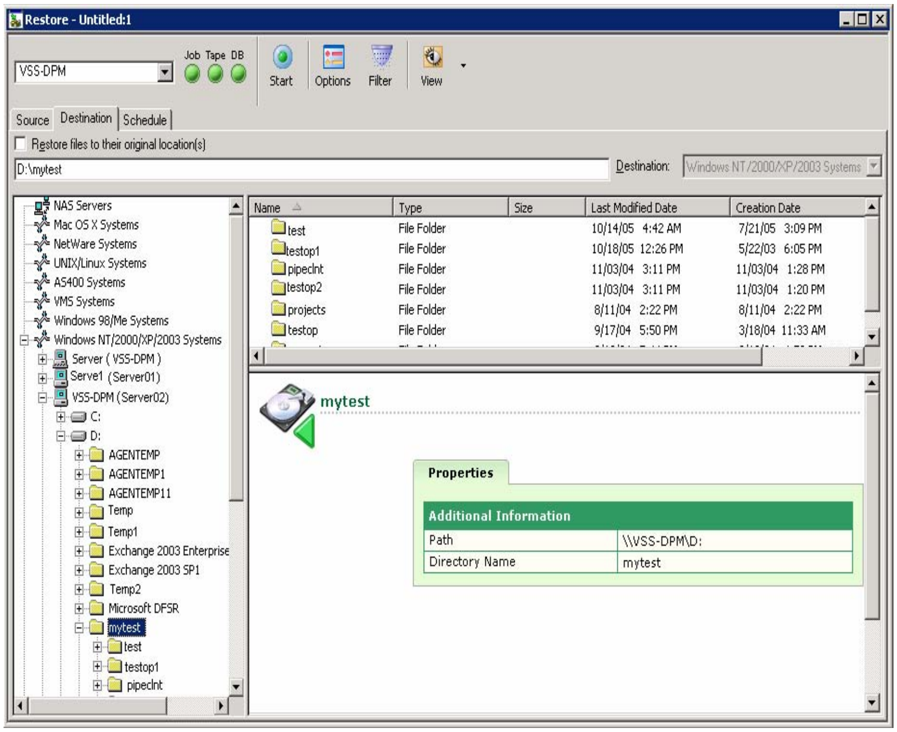
If you have lost files previously moved from your DPM server to the BrightStor ARCserve Backup server, you can recover these files by restoring the files and moving them back to your DPM protected server with the Client Agent for Windows.

Recover From BrightStor ARCserve Backup Server

Use the following steps to recover DPM-protected data from a BrightStor ARCserve Backup server:

1. Log on to the administrative BrightStor ARCserve Backup workstation as an administrative user.
2. Ensure that the volume you want to restore to is present.
3. Launch the Restore Manager.
4. Select the Restore by Tree method or Restore by Session method on the Restore Manager Source tab.
5. Click the appropriate green box next to the DPM Writer component you want to restore.

6. Clear the Restore files to their original location(s) check box, and specify the target path for your restore job on the Destination tab.



☐ Restore files to their original location(s)

D:\mytest

Destination: Windows NT/2000/XP/2003 Systems

Name	Type	Size	Last Modified Date	Creation Date
test	File Folder		10/14/05 4:42 AM	7/21/05 3:09 PM
testop1	File Folder		10/18/05 12:26 PM	5/22/03 6:05 PM
pipeclnt	File Folder		11/03/04 3:11 PM	11/03/04 1:28 PM
testop2	File Folder		11/03/04 3:11 PM	11/03/04 1:20 PM
projects	File Folder		8/11/04 2:22 PM	8/11/04 2:22 PM
testop	File Folder		9/17/04 5:50 PM	3/18/04 11:33 AM

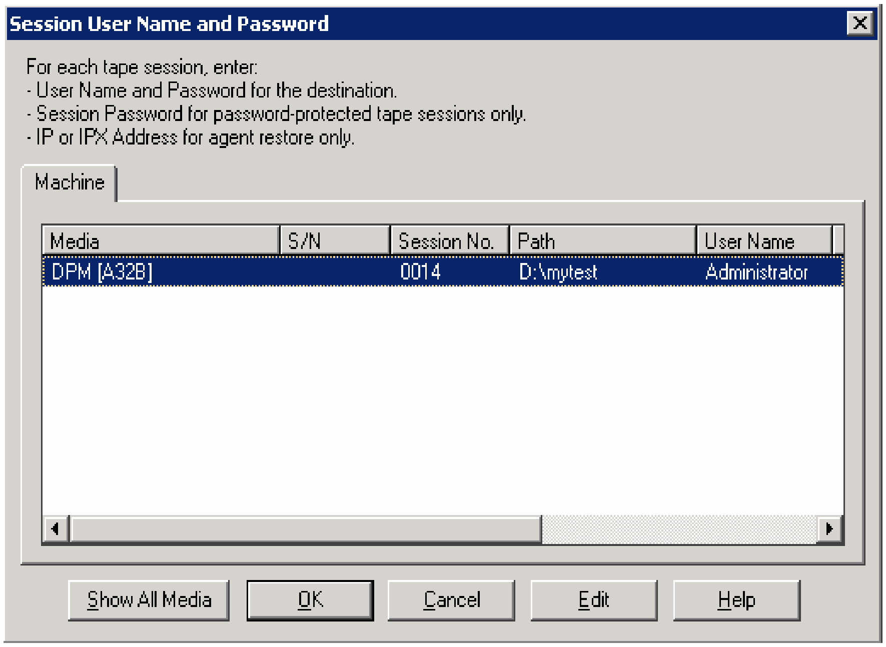
Properties

Additional Information	
Path	\\VSS-DPM\D:
Directory Name	mytest

7. Select the appropriate Repeat Method on the Schedule tab.

8. Click Start.

   The Session User Name and Password dialog appears.



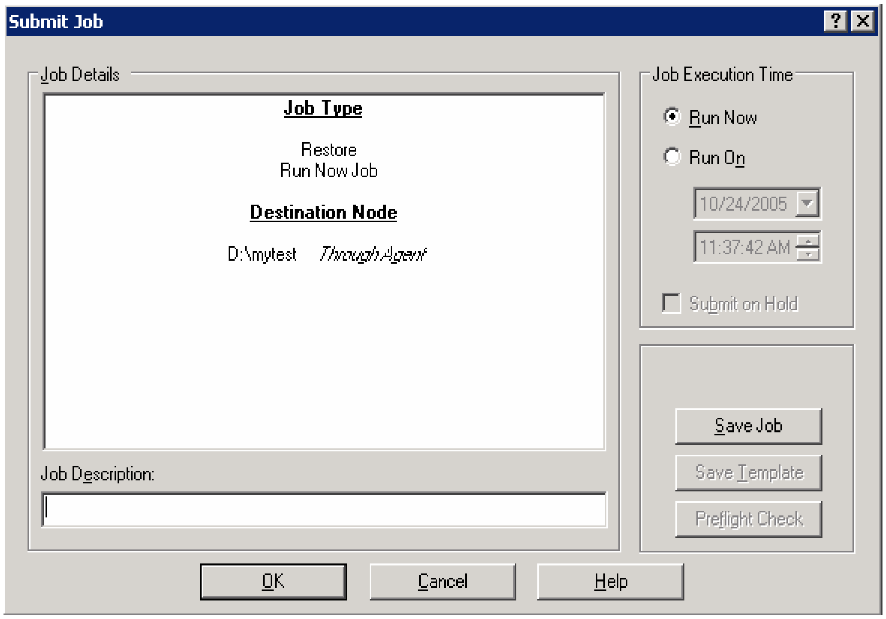
Session User Name and Password

For each tape session, enter:
- User Name and Password for the destination.
- Session Password for password-protected tape sessions only.
- IP or IPX Address for agent restore only.

Media	S/N	Session No.	Path	User Name
DPM [A32B]		0014	D:\mytest	Administrator

9. Edit or confirm the information in the Session User Name and Password dialog and click OK.

   The Submit Job dialog appears.



Submit Job

Job Details

Job Type

Restore
Run Now Job

Destination Node

D:\mytest *Through Agent*

Job Description:

Job Execution Time

● Run Now
○ Run On
10/24/2005
11:37:42 AM
□ Submit on Hold

10. Select the appropriate Job Execution Type. You can select one of the following:

    - **Run Now:** The restore job starts immediately
    - **Run On:** Enter the date and time to start the restore job

11. Click OK.

    You can monitor the job's progress using the Job Status Manager.

    Note: For more information about the Job Status Manager, see the *Administrator Guide*.

12. Launch Windows Explorer, browse to the location to which you restored the files, and drag and drop the restored files to the DPM protected server.

Server Data Loss

To protect your servers from disaster, you must have installed the BrightStor ARCserve Backup Disaster Recovery Option on the BrightStor ARCserve Backup server, created the necessary media before a disaster occurs, and performed a full backup. We strongly recommend that you create a disaster recovery plan.

To recover successfully after a disaster, you must create disaster preparation materials before the disaster strikes. If you do not prepare these materials, you cannot recover your systems. For more information about the Disaster Recovery Option, see the *Disaster Recovery Option Guide*.

Create a Disaster Recovery Plan

As part of your disaster recovery preparations, you should develop a disaster recovery plan. To create and test your plan, complete the following steps:

1. Create a set of disaster preparation materials to be kept off site. Follow the instructions in the subsequent sections of this guide to complete this step.
2. Set up a test server with a similar configuration to your original server.
3. Simulate a recovery on your test server by following the disaster recovery instructions in this guide.

DPM Protected Server Loss

If you lose a DPM protected server, you must rebuild it. If you have installed the BrightStor ARCserve Backup Client Agent for Windows and the Disaster Recovery Option on the server and have performed a full file system backup, the disaster recovery process is simple.

You can perform a disaster recovery using the BrightStor ARCserve Backup Disaster Recovery Option by booting from recovery media and providing a disk with critical server configuration information that can be created from the BrightStor ARCserve Backup Manager.

The restore process restores the system and boot volumes and brings the system to the state it was in when the full backup was performed.

If the system did not have the Client Agent for Windows or a full backup, it must be manually rebuilt to its previous configuration, the Microsoft DPM file agent must be installed, and the files in the DPM server must then be restored.

For more information on disaster recovery, see the *Administrator Guide* and the *Disaster Recovery Option Guide*.

DPM Server Loss

Restoring the DPM server after a loss of data is similar to recovering a DPM protected server. The key difference is that you must restore the DPM databases and DPM replicas from the BrightStor ARCserve Backup server after you have restored the operating system on the DPM server.

For more information about the Disaster Recovery Option, see the *Disaster Recovery Option Guide*.

Recover DPM Servers

Use the following steps to recover a DPM server using BrightStor ARCserve Backup, the Agent for DPM, and the Disaster Recovery Option:

1. Recover the operating system of DPM server using the Disaster Recovery Option.

   For information about the disaster recovery process, see the *Disaster Recovery Option Guide*.

2. Restart the system and verify that the operating system and critical system data have been restored.

3. Uninstall Microsoft Data Protection Manager 2006 using Add or Remove Programs and choose either the Remove Data or Retain Data option in the Uninstall Options dialog.

   When the uninstallation process finishes, click Close.

4. Uninstall the following DPM prerequisite software using Add or Remove Programs. You must uninstall these programs in the following sequence:

   a. SQL Server 2000 Reporting Services

   b. Internet Information Services (IIS)

   c. Microsoft SQL Server 2000 (MICROSOFT$DPM$)

5. Reboot your computer after all of the programs have been uninstalled.

6. Reinstall Microsoft DPM.

   Ensure that the DPM Writer service is started. Check the status of the service using Windows Administrative Tools\Services.

7. Launch the BrightStor ARCserve Backup Manager and follow the standard restore procedures to restore the Microsoft DPM Database DPMDB and Database ReportServer to their original locations.

8. Execute the following command from C:\Program Files\Microsoft Data Protection Manager\DPM\bin\ from a DOS prompt:

   ```
   DpmSync -Sync
   ```

   If your DPM Server is not installed in its default location, check the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Setup\DatabasePath to determine the installation path.

   Note: If your DPM Server is monitored in Microsoft Operations Manager 2005 (MOM), after you restore the DPM database, you must synchronize the alerts in MOM with those on the DPM Server. For more information, see the Data Protection Manager 2006 Management Pack Guide on the Microsoft TechNet site MOM 2005 Management Pack Guides (http://go.microsoft.com/fwlink/?linkid=50206).

9. Launch the DPM Administrator Console and add the disks to the storage pool.

   Note: You need not perform this step if your operating system has the access to the disks that were originally allocated for DPM.

10. Launch BrightStor ARCserve Backup Manager, and follow the standard restore procedures to restore the DPM replicas to their original locations.

11. From the DPM Administrator, perform Verification with Consistency Check on each replica after recovering all of your protected resources.

    For information about these procedures, see the *Microsoft DPM* documentation.

DPM and DPM Protected Servers Loss

If you suffer wide-scale data loss, you lose your DPM server and one or more DPM protected servers at the same time. Use one of the following options under such circumstances:

- Recover your DPM server first and use it to stage the recovery of your DPM protected servers.
- Recover one or more DPM protected servers directly and restore the DPM server when the critical servers are back online.

Recover the DPM Server First

Recovering the DPM server first is a slower process. You must first recover multiple replicas to the DPM server and then restore the data to the DPM protected servers.

The main advantage of this option is that it ensures the protection of your DPM protected servers as soon as they are brought back online. However, this method requires that you have all of your usual disk storage capacity for the DPM server. In the event of a wide-scale outage, you may not have spare disk resources on hand. In addition, if you have a large number of servers to rebuild, the process may be slowed.

Recover the DPM Protected Server First

Recovering at least some of DPM protected servers first is quicker than recovering the DPM server first. BrightStor ARCserve Backup offers built-in integration with DPM, to help you easily restore your production data from tape directly through the Client Agent for Windows running on the DPM protected server without requiring the DPM server to be running. This response time is often critical when you have mission-critical servers and data to be restored.

BrightStor ARCserve Backup Server Loss

Recovering from BrightStor ARCserve Backup server loss is similar to recovering from DPM protected server loss. The recovery features provided by the BrightStor ARCserve Backup Disaster Recovery Option allow you to recover your backup server automatically. However, you need to ensure the following before a server failure:

1. Install the BrightStor ARCserve Backup Disaster Recovery Option on the server.
2. Configure an alternate location for storing Disaster Recovery information when you setup your server.
3. Perform regular full backups of the backup server.

   Note: For more information on performing regular full backups, see the *Disaster Recovery Option Guide*.

Reports

BrightStor ARCserve Backup provides several types of reports. You can access these reports from the BrightStor ARCserve Backup Report Manager. The Report Manager provides several functions to help manage both reports and logs. For more information about reports, see the *Administrator Guide*.

Appendix A: Troubleshooting

This appendix provides troubleshooting information to help you identify and resolve problems you may encounter when using BrightStor ARCserve Backup and the Agent for Microsoft DPM. To help you quickly find the information you need, this appendix includes error messages and possible reasons and solutions for these messages.

Error Messages

This section explains the most common error messages for the Agent for Microsoft DPM.

Activity Log

Many of the actions to resolve error conditions advise you to check the BrightStor ARCserve Backup Activity log. The Activity log contains comprehensive information about the operations performed by BrightStor ARCserve Backup. It provides an audit trail of all BrightStor ARCserve Backup activity for every job that is run. You can scan this log whenever necessary to see if any errors have occurred. The log is available from the Job Status Manager. For more information about using the Activity log, see the Administrator Guide.

E3243

Failed to communicate with client agent

Reason:

The connection with the client agent was broken.

Action:

Restart the BrightStor Universal Agent service and retry the operation.

12502

The volume shadow service provider has reported a bad state for the operation

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12503

An attempt was made to register an ID for a volume shadow service provider that is already registered

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12504

An attempt was made to use a provider ID that does not correspond to a registered volume shadow service provider

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12505

The volume shadow service provider vetoed an operation. The provider logged the error in the event log

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12506

The volume shadow service provider is in use, please try again later

Reason:

Another process is using the Volume Shadow Service Provider.

Action:

Retry the operation.

12507

The volume shadow service provider is unable to find an object that has been selected. This could be a volume, writer, component, etc.

Reason:

The selected Volume, Writer or Component is not available to the Volume Shadow Service Provider.

Action:

Check the Activity log and the Windows Event log for additional information.

12508

A volume shadow service provider can not be found to support one of the volumes selected directly or indirectly through a writer

Reason:

This is an internal Microsoft Volume Shadow Copy Service error. A volume has been selected that cannot be incorporated into a shadow copy.

Action:

Check the Activity log and the Windows Event log for additional information.

12509

The object is a duplicate. An attempt was made to add a component with the same logical path and component name or private metadata has already been written

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12510

The volume shadow service provider being used does not support one of the volumes selected directly or indirectly through a writer

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12511

The volume shadow service provider had an unexpected error. The error code is logged in the error log

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12512

The volume shadow service provider reports that one of the XML documents is invalid or has become corrupted. Please refer to the event log for details

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12513

The volume shadow service provider is unable to load the XML document passed in the bstrXML argument or it is not valid, that is, either it is not a correctly formed XML string or it does not match the schema

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12514

The maximum number of volumes has been added for the shadow copy set. At least one of the specified volumes could not be added to the shadow copy set

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12515

The volume shadow service provider reported a flush writes timeout

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12516

The volume shadow service provider reported a hold writes timeout

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12517

The volume shadow service provider reported an unexpected writer error

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12518

The volume shadow service provider was unable to complete the operation as a shadow copy was in progress. Please try again later

Reason:

Another process is creating or using a shadow copy.

Action:

Retry the operation when the other process has completed.

12519

The volume shadow service provider was unable to complete the operation as the maximum number of snapshots has been reached

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Delete one or more snapshots and retry the operation.

12520

The volume shadow service infrastructure is not operating properly. Check that the Event Service and VSS have been started, and check for errors associated with those services in the event log

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information. Verify that the Event Service and VSS have been started, and then retry the operation.

12521

A selected volume shadow service writer is not responding

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12522

The writer has already been subscribed with the volume shadow service

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12523

The volume shadow service provider reported an unsupported context

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12524

The volume shadow service provider was unable to complete the operation as the volume is in use

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12525

The volume shadow service provider was unable to complete the operation as the maximum number of difference area associations has been reached

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12526

The volume shadow service provider was unable to complete the operation as it has insufficient storage space. Please check the volume shadow service use limit

Reason:

This is an internal Microsoft Volume Shadow Copy Service error. This error message may indicate that the service has insufficient space in which to store the shadow copy.

Action:

Increase the available disk space on a local NTFS drive and retry the operation.

12527

The volume shadow service provider reported that no volume shadow copies were imported

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12528

The volume shadow service provider reported that only some volume shadow copies were imported

Reason:

This is an internal Microsoft Volume Shadow Copy Service error.

Action:

Check the Activity log and the Windows Event log for additional information.

12565

An unexpected error has occurred. Error Code *(code)*

Reason:

The Volume Shadow Copy Service has generated an unexpected error.

Action:

Check the Activity log and the Windows Event log for additional information. If this error persists, contact Customer Support.

12567

The addition of the components failed in the restore

Reason:

One or more of the components specified to be restored have caused a failure.

Action:

Check the Activity log and the Windows Event log for additional information. Log entries may identify the component and the reason for the failure.

12568

Unable to find the user selected options

Reason:

One or more of the components selected to be restored do not exist on the destination computer.

Action:

Ensure that all of the Writers required for the restore are running on the destination computer. To verify, browse through the Backup Manager to view all the Writers, or run the VSSADMIN LIST command from a command window to list all installed Writers.

> **Note:** For more information about the VSSADMIN command, see the Windows Server 2003 documentation.

12569

Unable to write data to the files list

Reason:

A write request to the file list has failed.

Action:

Ensure that there is sufficient disk space available and retry the operation.

12570

Failed to back up file *(filename)*

Reason:

The specified file could not be backed up.

Action:

Retry the operation.

12571

Writer *(writer)* does not exist on the system

Reason:

The backup job includes the specified Writer but the Writer is not currently running on the source computer.

Action:

Either modify the job to remove the Writer or ensure the Writer is running on the source computer.

12572

The writer's constructed file path exceeds MAX_PATH

Reason:

The internal representation of the Writer name has exceeded the maximum allowed length.

Action:

You cannot back up this Writer.

12573

An attempt was made to construct a path name with an empty root path

Reason:

An internal error has occurred.

Action:

If this error persists, contact Customer Support.

12574

The path "%1" has a bad format

Reason:

An internal error has occurred.

Action:

If this error persists, contact Customer Support.

12575

Unable to restore writer *(writer)*

Reason:

The specified Writer could not be restored.

Action:

Check the Activity log and the Windows Event log for additional information.

12576

Unable to restore Writer, File *(file)*

Reason:

The restore process is not able to restore the specified file.

Action:

You may have to perform application-specific procedures before you can restore the specified file. Contact the supplier of the Writer for assistance.

12577

Component *(component)* is not selectable

Reason:

The specified Component cannot be independently selected for restore.

Action:

Select either the whole Writer or another Component that includes this one.

12578

Unable to find the component set for component *(component)*

Reason:

The parent Component cannot be found for the specified Component. The Component selected for restore was not specifically selected at the time of backup and no parental relationship to the selected Component can be found.

Action:

Restore the whole Writer or restore the Component to an alternate location.

12581

This writer has a custom restore. Please contact the writer provider

Reason:

You cannot directly restore a Writer that specifies a custom restore method. User intervention is required to restore this writer.

Action:

Contact the supplier of the Writer for the procedure needed to restore the data.

12582

This writer *(writer)* has reported an unknown state

Reason:

An error has occurred in the Writer.

Action:

Check the Windows Event log for errors related to the Writer. Try restarting the Writer and retry the operation.

12583

This VSS writer has reported a failure on an identification event

Reason:

The Writer vetoed the shadow copy creation process at the Writer Identification state.

Action:

Check the Windows Event log for errors related to the Writer.

12584

This VSS writer *(writer)* has reported a failure on a prepare for backup event

Reason:

The specified Writer vetoed the shadow copy creation process during the Backup Preparation state. This error may be due to inconsistencies in the backup method selected on the Writer Options dialog for a particular Writer and the backup methods that are actually supported by the Writer.

Action:

Check the Windows Event log for errors related to the Writer.

12585

This VSS writer *(writer)* has reported a failure on a prepare for snapshot event

Reason:

The specified Writer vetoed the shadow copy creation process during the Prepare For Snapshot state.

Action:

Check the Windows Event log for errors related to the Writer.

12586

This VSS writer *(writer)* has reported a failure on a freeze event

Reason:

The specified Writer vetoed the shadow copy creation process during the Freeze state.

Action:

Check the Windows Event log for errors related to the Writer.

12587

This VSS writer *(writer)* has reported a failure on a thaw event

Reason:

The specified Writer vetoed the shadow copy creation process during the Thaw state.

Action:

Check the Windows Event log for errors related to the Writer.

12588

This VSS writer *(writer)* has reported a failure on a post snapshot event

Reason:

The specified Writer vetoed the shadow copy creation process during the PostSnapshot state.

Action:

Check the Windows Event log for errors related to the Writer.

12589

This VSS writer *(writer)* has reported a failure on a backup complete event

Reason:

The shadow copy has been created and the specified Writer failed during the BackupComplete state. The Writer should save information about this failure to the error log.

Action:

Check the Windows Event log for errors related to the Writer.

12590

This VSS writer *(writer)* has reported a failure on a pre restore event

Reason:

The specified Writer failed during the PreRestore state.

Action:

Check the Windows Event log for errors related to the Writer.

12591

This VSS writer *(writer)* has reported a failure on a post restore event

Reason:

The specified Writer failed during the PostRestore state.

Action:

Check the Windows Event log for errors related to the Writer.

12592

This VSS writer *(writer)* has reported a failure on a backup shutdown event

Reason:

The specified Writer failed during the shutdown of the backup application.

Action:

Check the Windows Event log for errors related to the Writer.

12593

The shadow copy contains only a subset of the volumes needed by the writer to correctly back up the application component

Reason:

The shadow copy does not include all the required volumes for the associated Writer.

Action:

Check the Activity log and Windows Event log for errors related to the Writer.

12594

The writer ran out of memory or other system resources

Reason:

This is an internal error generated by the Writer.

Action:

Check the Activity log and Windows Event log for errors related to the Writer. Restarting the Writer or rebooting the system may resolve the problem.

12595

The writer operation failed because of a time-out between the Freeze and Thaw events

Reason:

This is an internal error generated by the Volume Shadow Copy Service and indicates that the Writer was unable to comply in time.

Action:

Check the Activity log and Windows Event log for errors related to the Writer.

12596

The writer failed due to an error that would likely not occur if the entire backup, restore, or shadow copy creation process was restarted

Reason:

This is an internal error generated by the Writer.

Action:

Check the Activity log and Windows Event log for errors related to the Writer. Retry the operation.

12597

The writer operation failed because of an error that might recur if another shadow copy is created

Reason:

This is an internal error generated by the Writer.

Action:

Check the Activity log and Windows Event log for errors related to the Writer. Retry the operation.

12598

The writer is not responding

Reason:

The Writer is not responding to requests.

Action:

Check the Activity log and Windows Event log for errors related to the Writer. Ensure the Writer is running and retry the operation.

12599

An Error has occurred trying to create the browse manager

Reason:

An internal error is preventing the creation of the browse manager.

Action:

Restart the BrightStor ARCserve Backup services on the machine being browsed. If this error persists, contact Customer Support.

12601

Unable to find a file which meets the file descriptor *(file)*

Reason:

The Writer has included the specified file in the list of files to be backed up but the file does not exist.

Action:

The Writer may not be able to be restored correctly without the specified file. This error may indicate that the application data is in a bad state.

12602

Unable to back up writer *(writer)*

Reason:

An error has occurred that indicates that the specified Writer cannot be backed up.

Action:

Check the Activity log and Windows Event log for errors related to the Writer.

12603

The shadow copy does not exist

Reason:

An internal error has occurred that prevented the creation of a shadow copy.

Action:

Check the Activity log and the Windows Event log for additional information.

12604

Unable to get the writer from the VSS interface

Reason:

An internal error has occurred that prevented the Writer from being backed up.

Action:

Check the Activity log and the Windows Event log for additional information.

12605

The selected item is not a writer

Reason:

An internal error has indicated that the specified item is not a Writer.

Action:

Check the Activity log and the Windows Event log for additional information.

12606

Unable to get the selected writer options

Reason:

An internal error has prevented the selected Writers from being backed up.

Action:

Check the Activity log and the Windows Event log for additional information.

12607

The selected index is invalid

Reason:

An internal error has prevented the selected item from being backed up.

Action:

Check the Activity log and the Windows Event log for additional information.

Glossary

bare metal recovery

Bare metal recovery is the process of recovering data or rebuilding a computer after a catastrophic failure.

DPM Writer

DPM Writer is a Windows service that ensures its data is quiescent and stable-suitable for shadow copy and backup. It also collaborates with restores by unlocking files when possible and indicating alternate locations when necessary.

Microsoft Data Protection Manager 2006

Microsoft Data Protection Manager is a server software application that provides Windows NTFS file system based backup and recovery.

Microsoft Windows Server System

Microsoft Windows Server System is a portfolio of integrated server software products that provides the infrastructure for IT operations, application development and integration, security, and collaboration.

replica

Replica is the container that hosts the protected volumes or share folders of the DPM protected servers. Each replica represents a share folder or volume of a DPM protected server.

Virtual Tape Library (VTL)

VTL is a storage system that includes a disk, a processor, and software to emulate tape or a tape library.

Volume Shadow Copy Service (VSS)

VSS provides the backup infrastructure for Microsoft Windows Server 2003 and Microsoft Windows XP operating systems, and a mechanism for creating consistent point-in-time copies of data (shadow copies). Applications can continue to write data to the disk volume during the shadow copy creation process, eliminating the need to perform backups before or after business hours. Additionally, a volume copy backup lets you perform file restores, minimizing administrative overhead for basic restore operations.

Index